

FIG.1

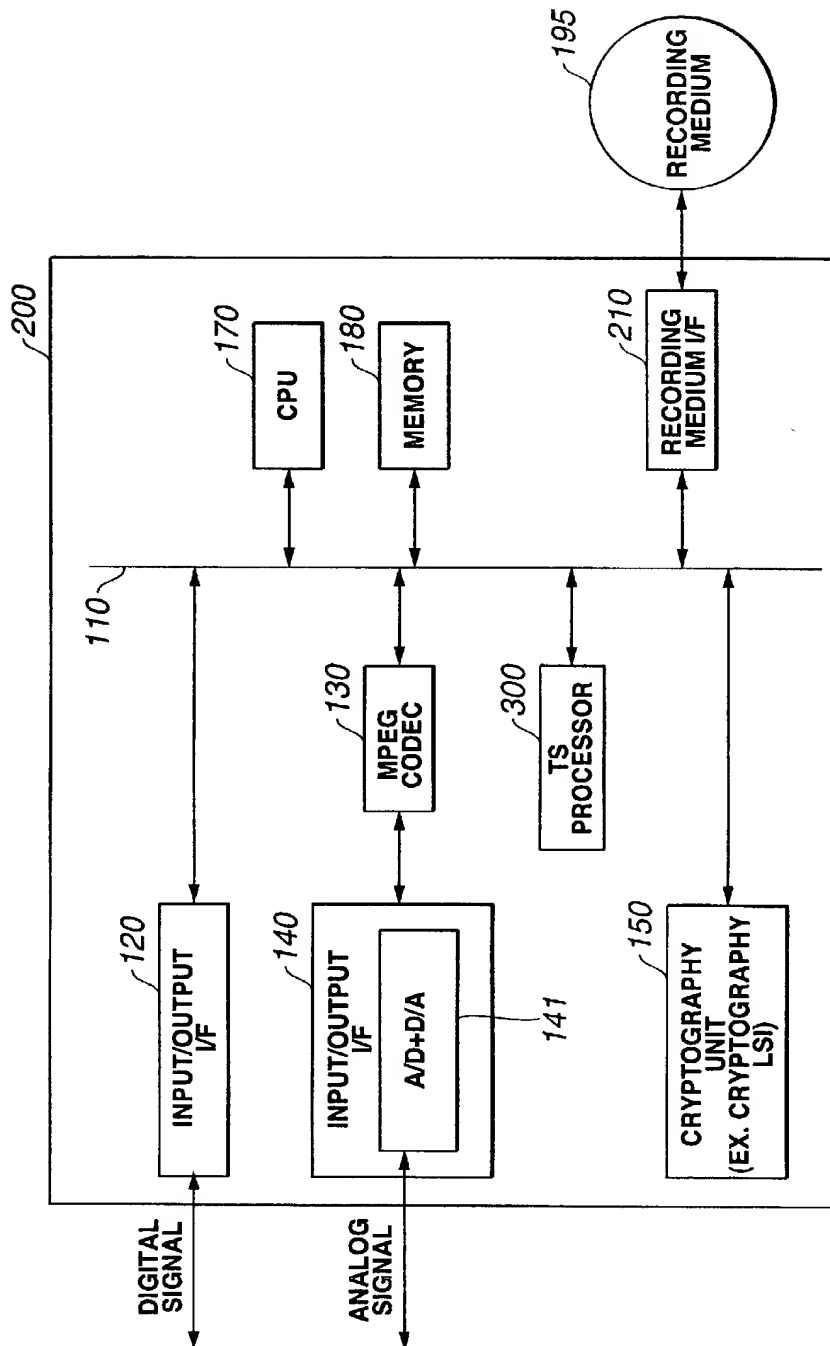


FIG.2

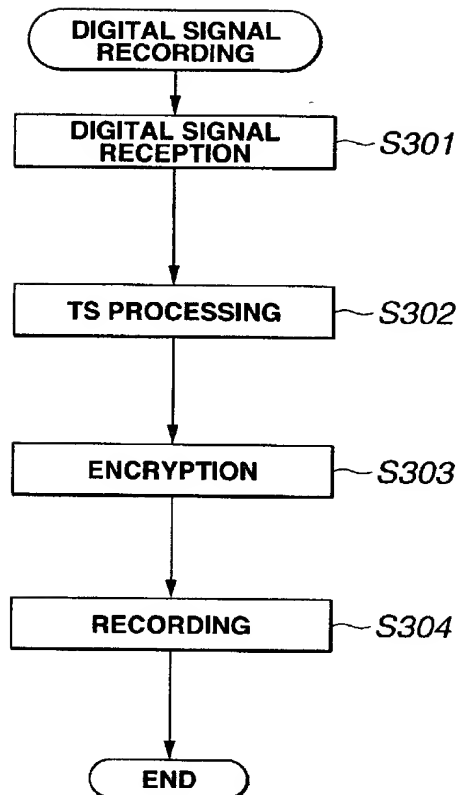


FIG.3A

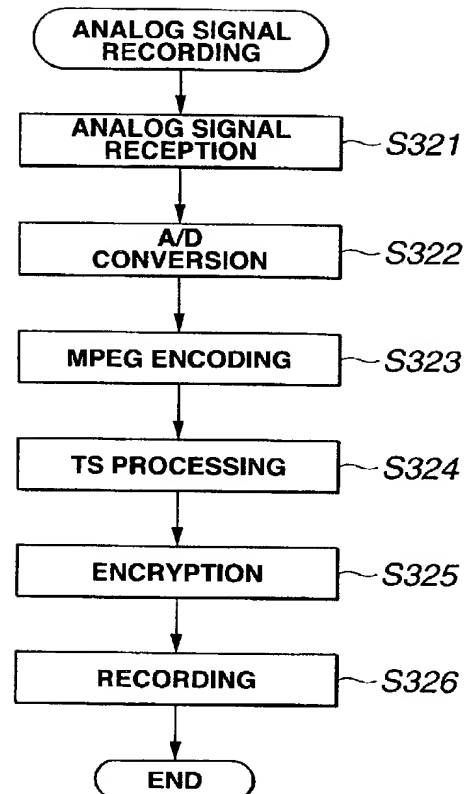


FIG.3B

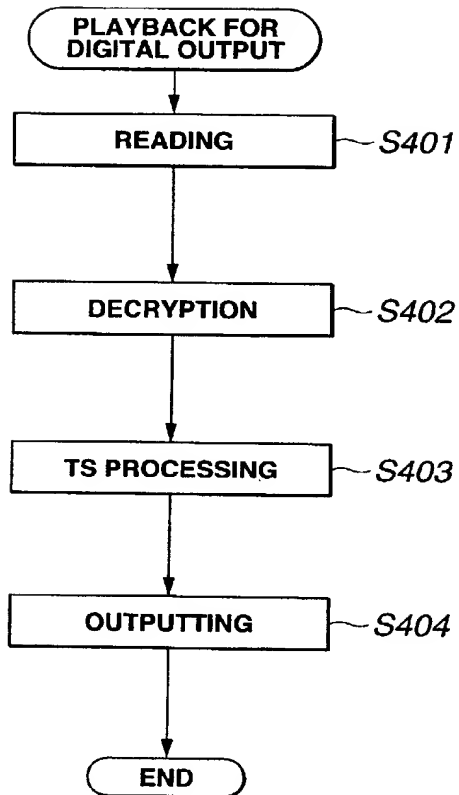


FIG.4A

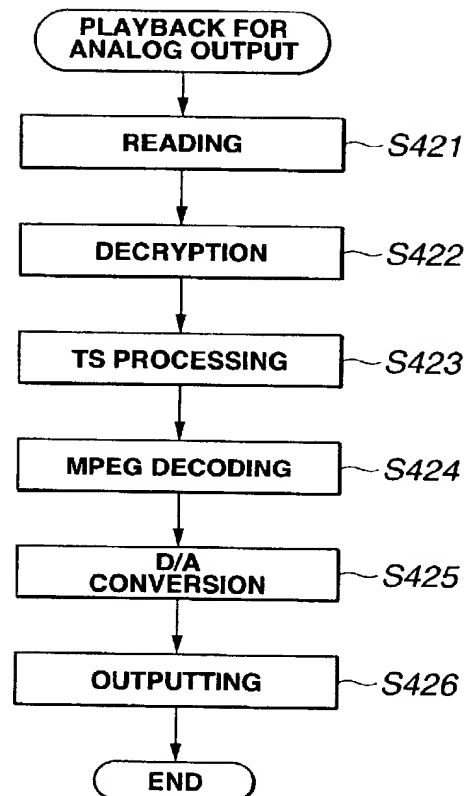
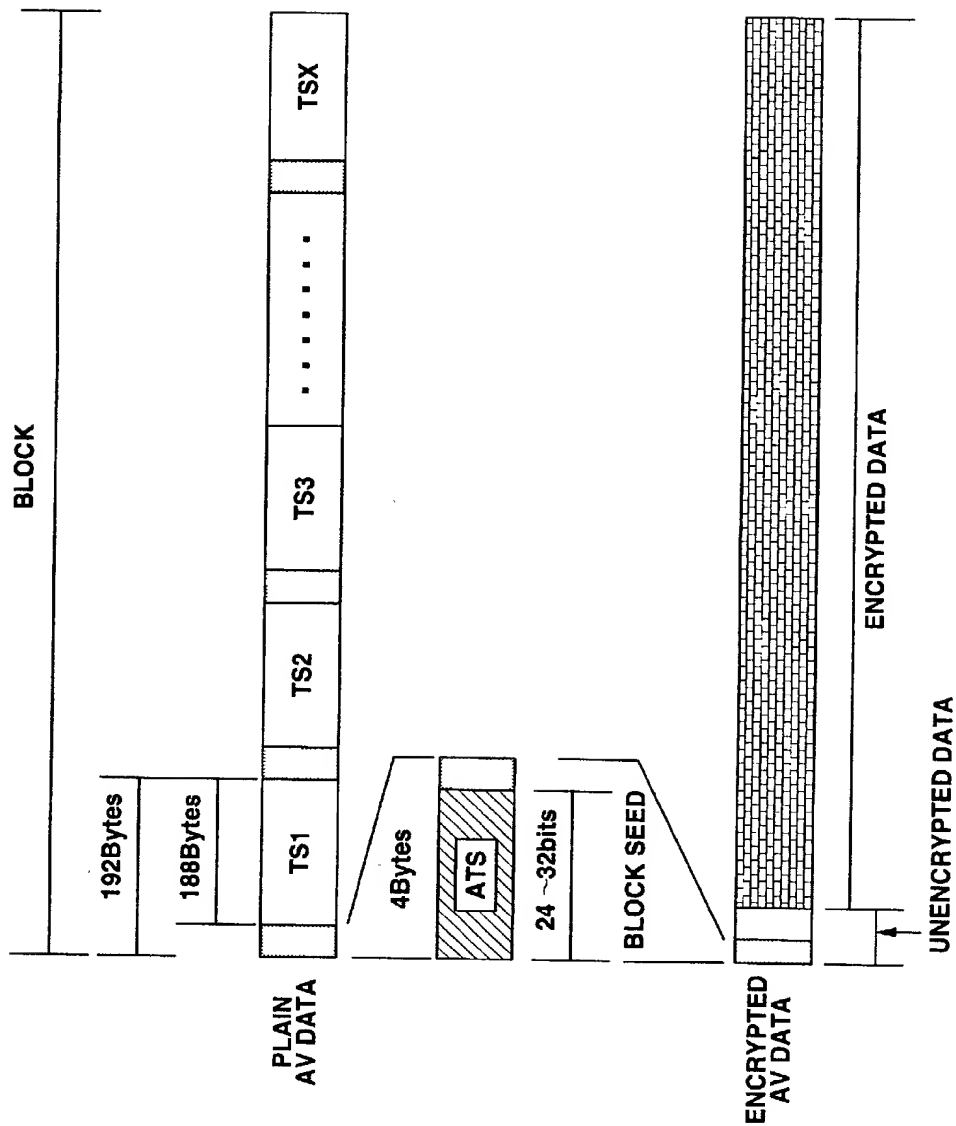


FIG.4B



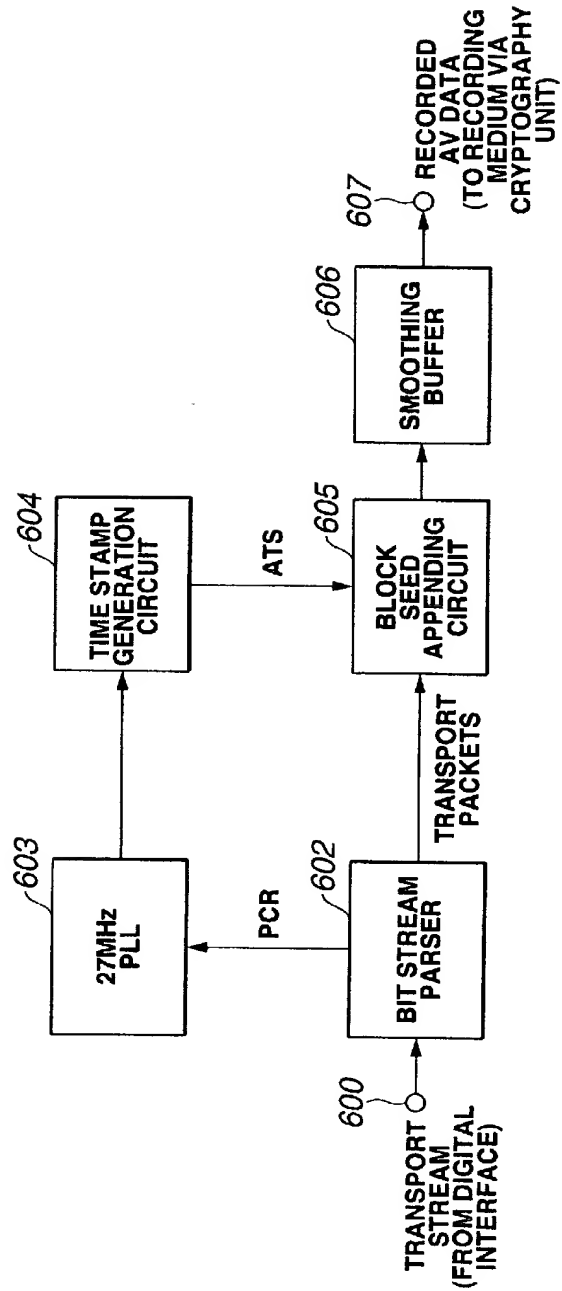


FIG. 6

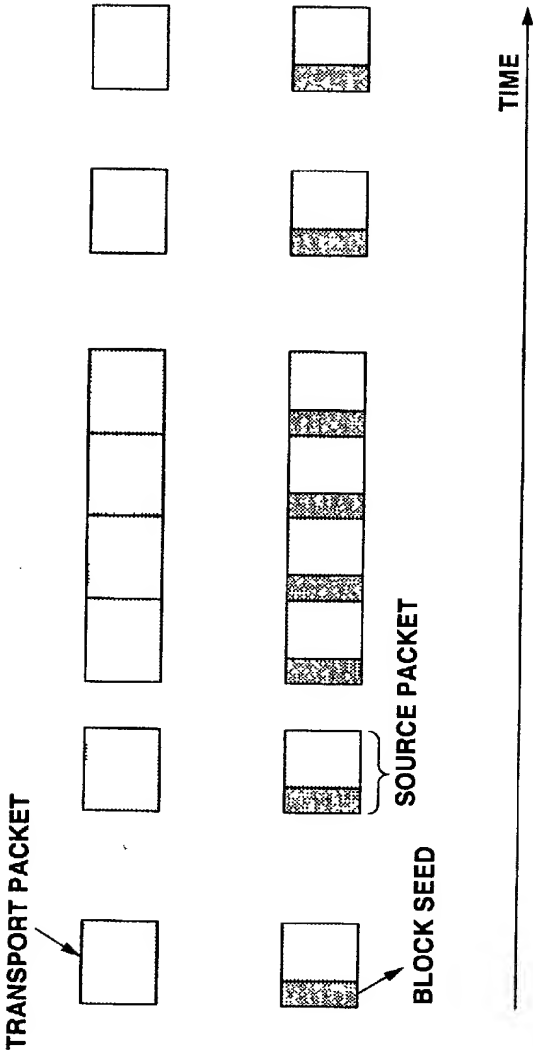


FIG.7A
INPUT
TRANSPORT
STREAM

FIG.7B
OUTPUT OF BLOCK
SEED APPENDING
CIRCUIT

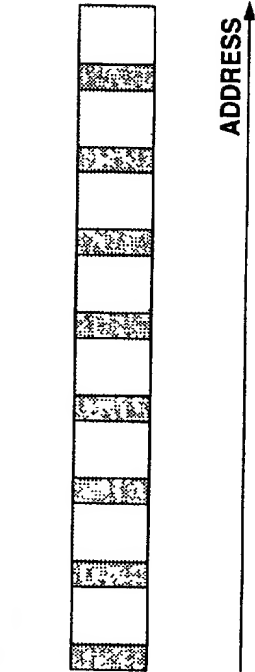


FIG.7C
AV DATA ON
RECORDING
MEDIUM



FIG. 8

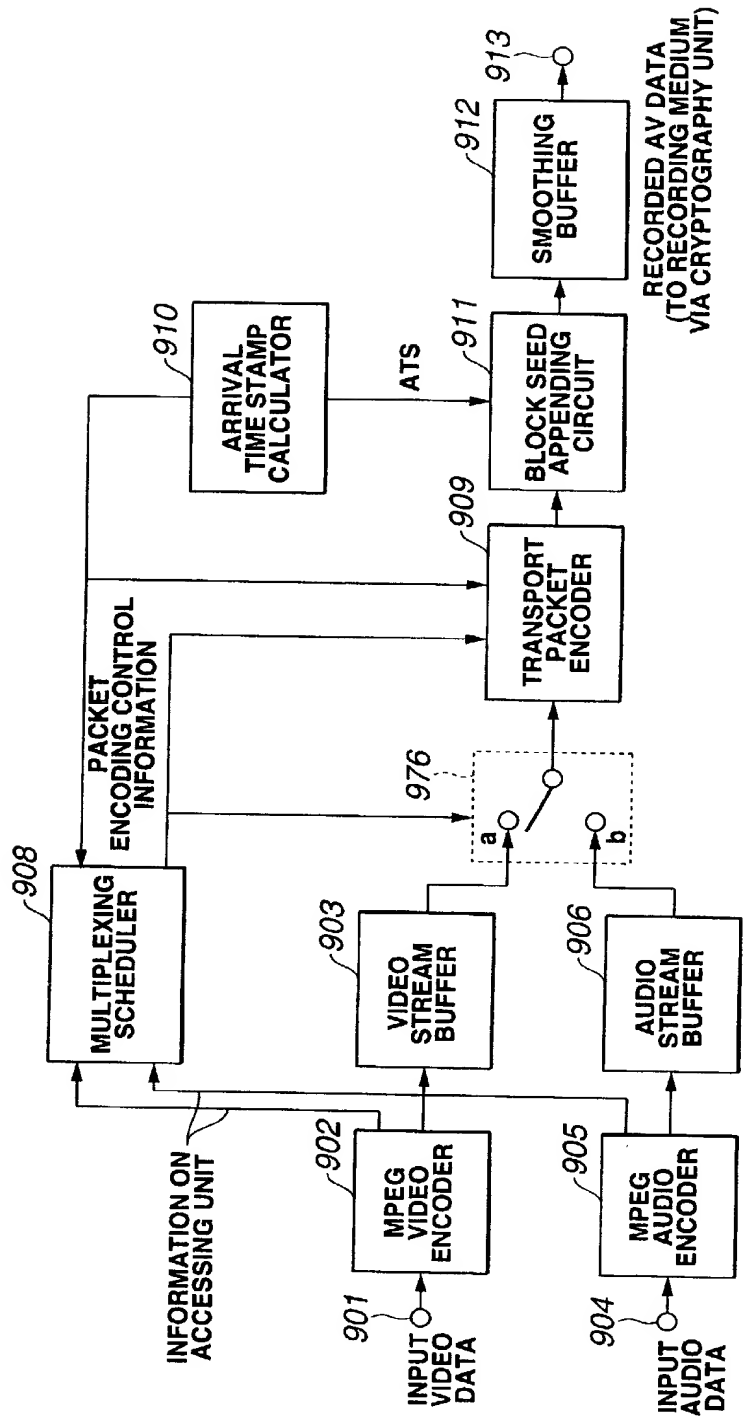


FIG.9

200003272

EXAMPLE 1: ATS OF 32BITS

ATS

**EXAMPLE 2:
ATS OF 30 BITS
AND CCI OF 2BITS**

ATS

151

**EXAMPLE 3:
ATS OF 24BITS,
CCI OF 2 BITS
AND OTHER
INFORMATION
OF 6 BITS**

ATS

100

OTHER INFORMATION

FIG. 10

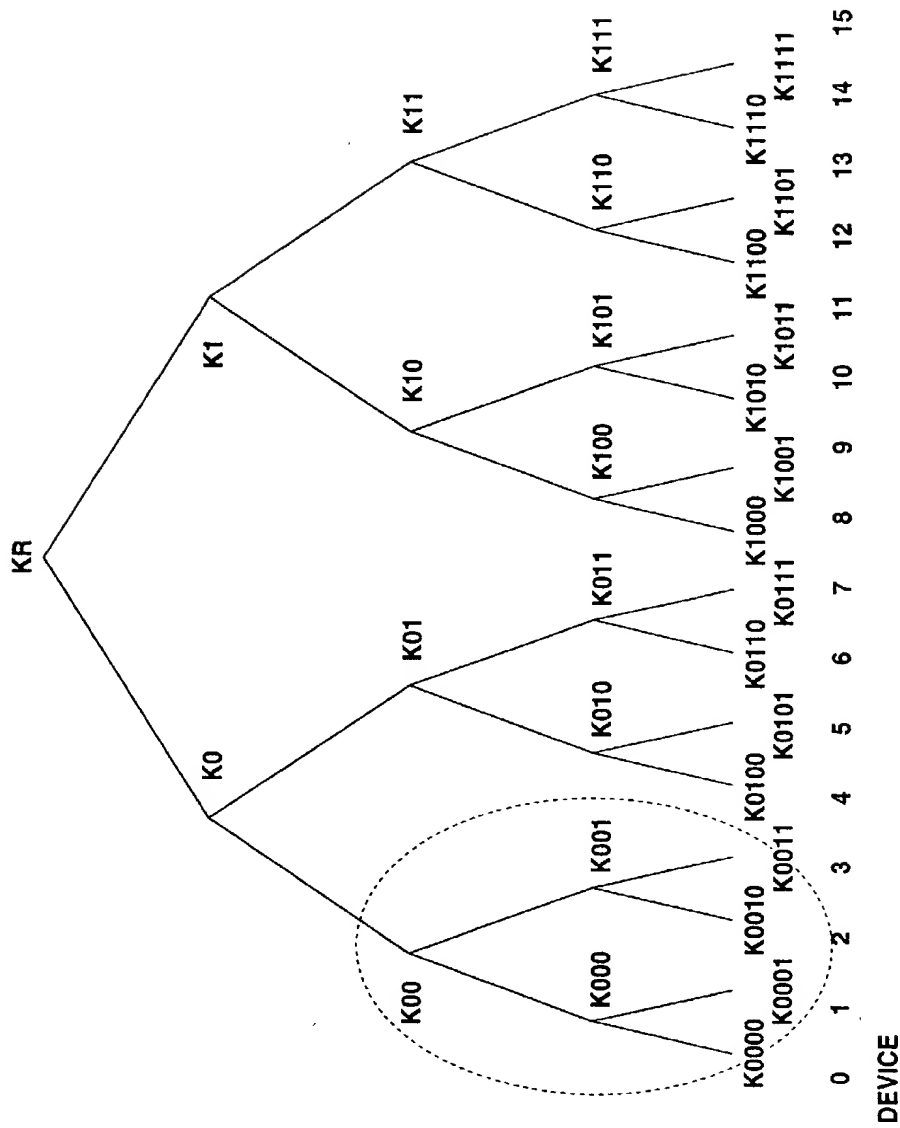


FIG. 11

GENERATION : t	
INDEX	ENCRYPTION KEY
0	$\text{Enc}(K(t)0, K(t)R)$
00	$\text{Enc}(K(t)00, K(t)0)$
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

FIG.12A

GENERATION : t	
INDEX	ENCRYPTION KEY
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

FIG.12B

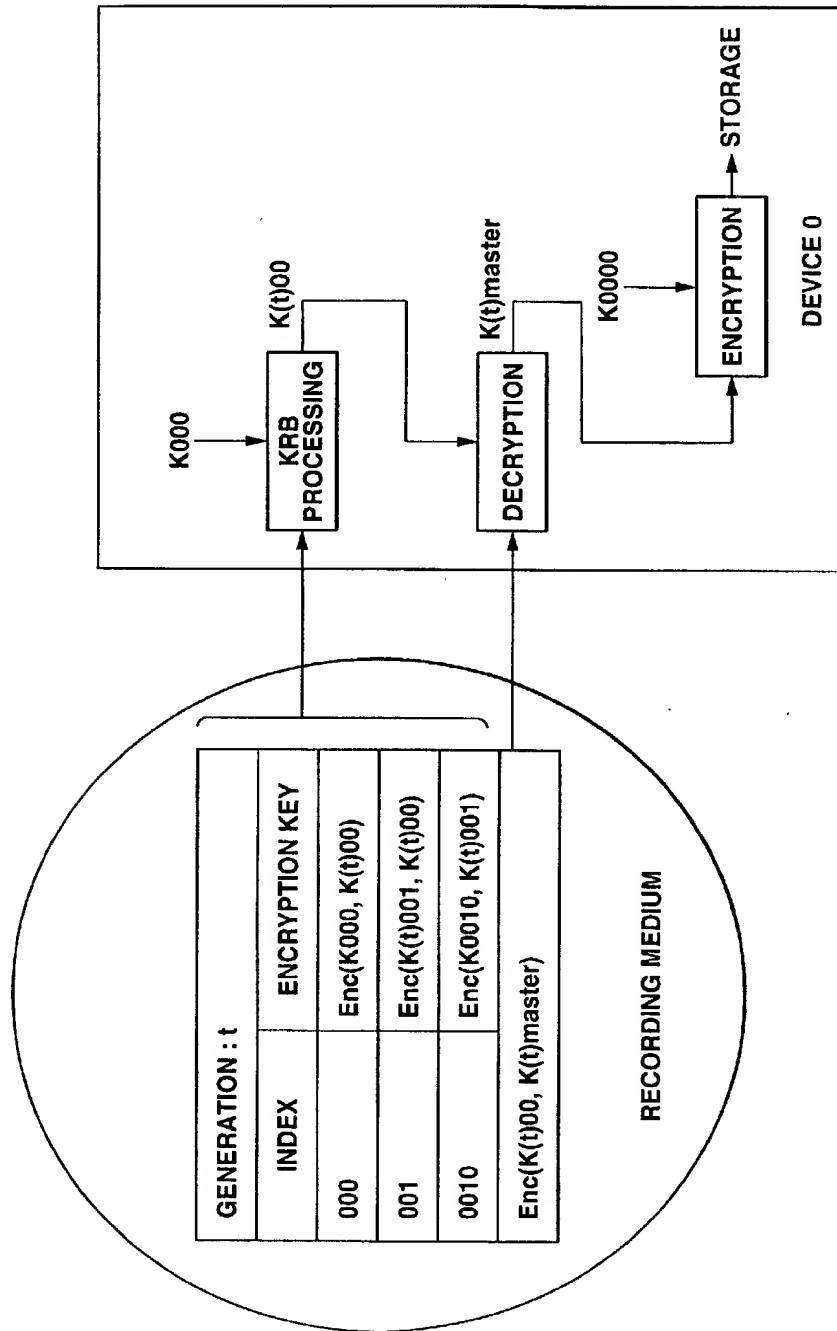


FIG.13

14/43

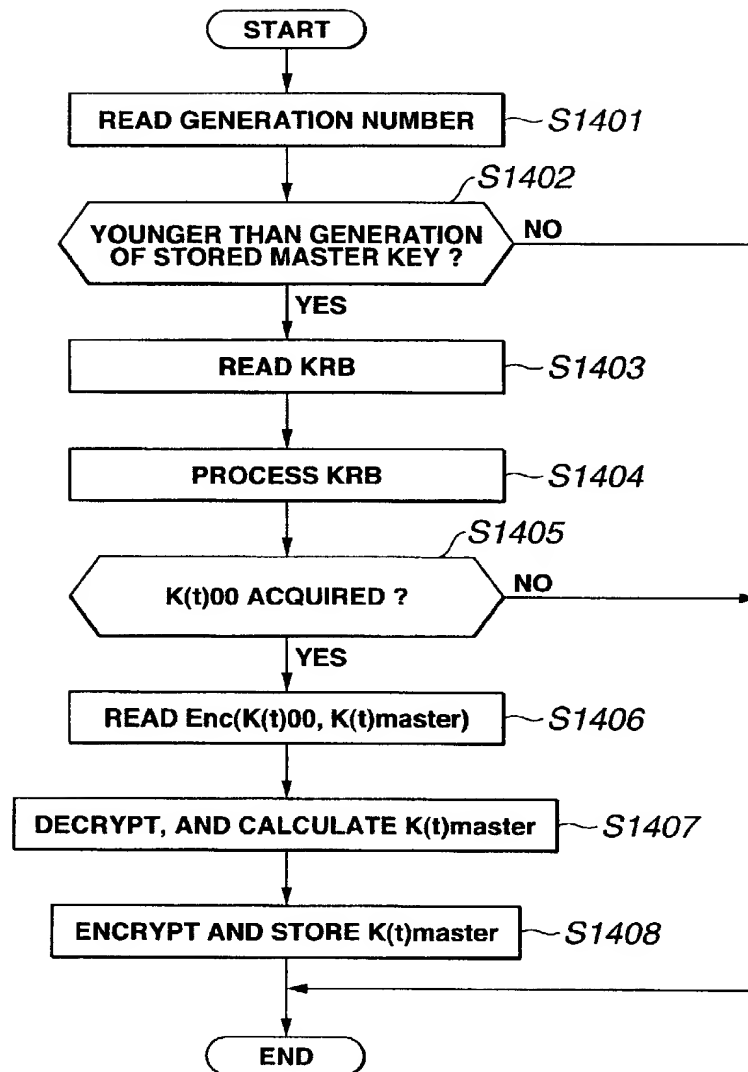


FIG.14

15/43

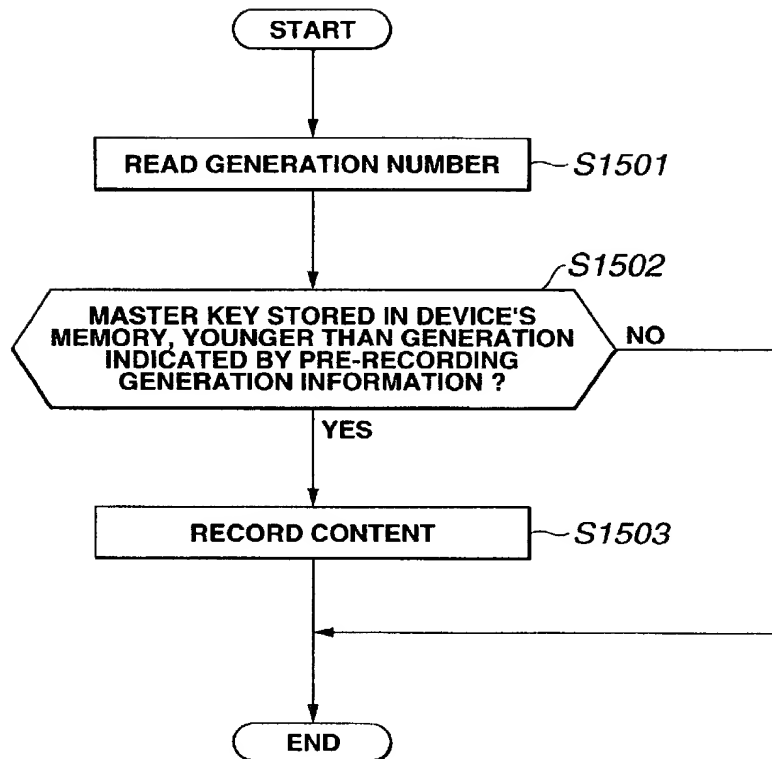
**FIG.15**

FIG. 16

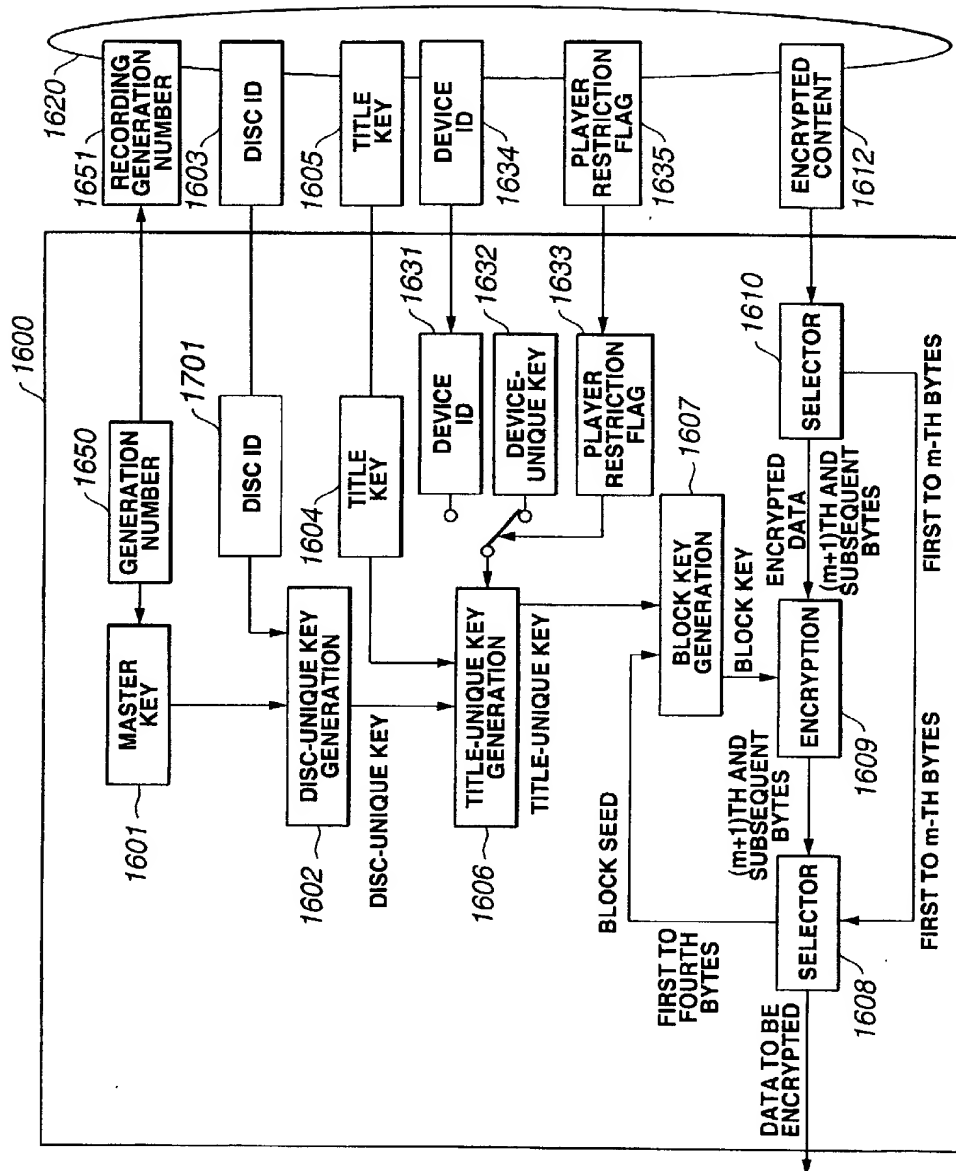


FIG.17

18/43

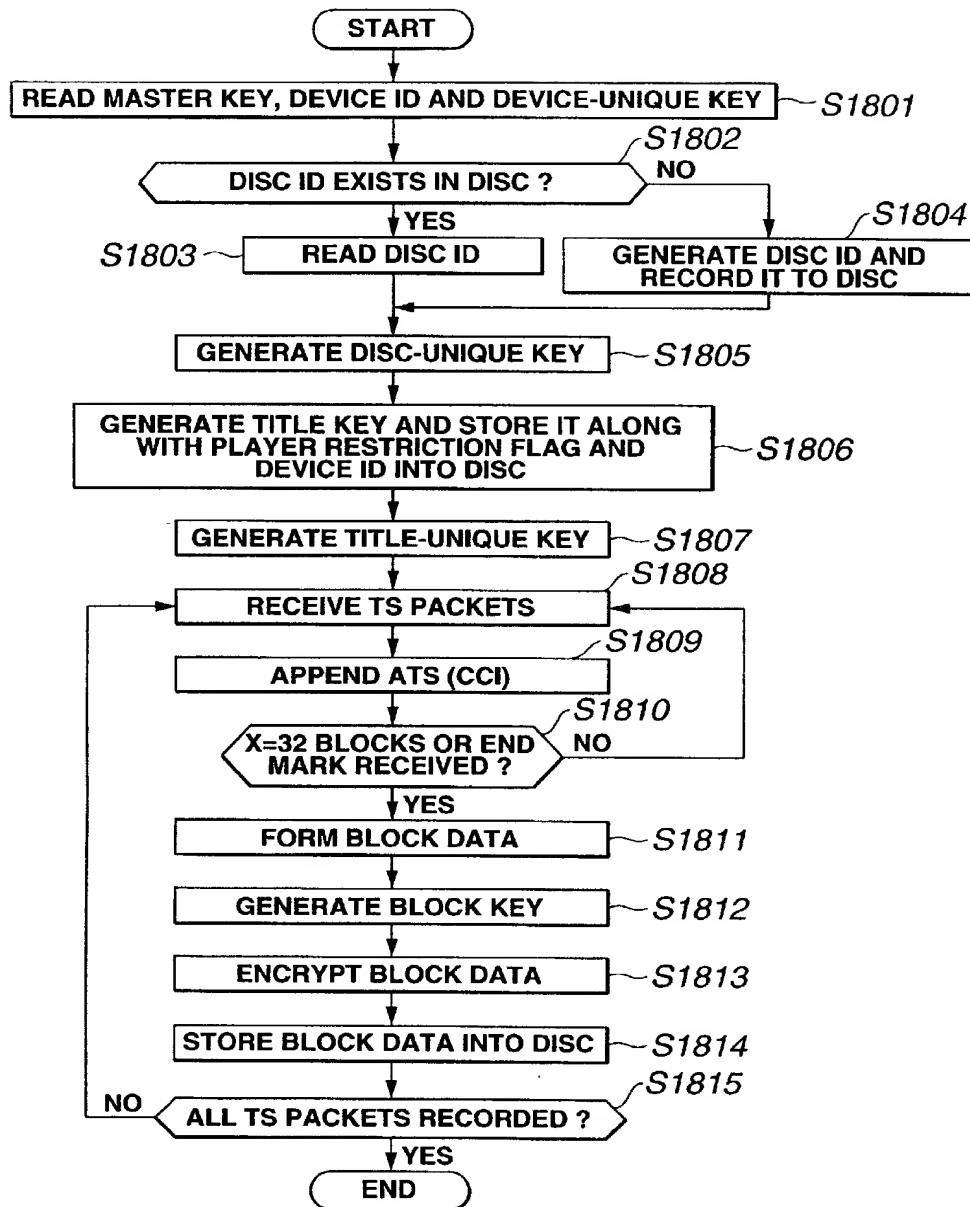


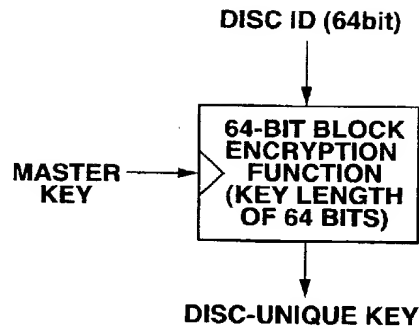
FIG.18

19/43

EXAMPLE 1

EXAMPLE OF DEVICE-UNIQUE
KEY GENERATION

INPUTS:
MASTER KEY (64BITS)
DISC ID (64BITS)



OUTPUTS:
DISC-UNIQUE KEY (64BITS)

EXAMPLE 2

MASTER KEY||DISC ID

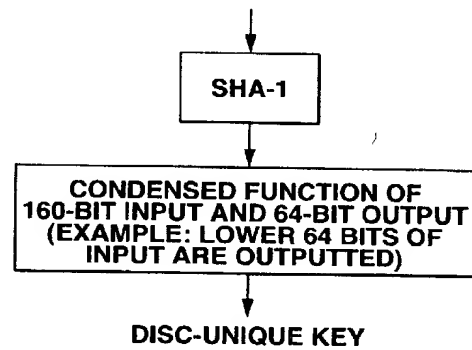


FIG.19

US 7,002,112 B2

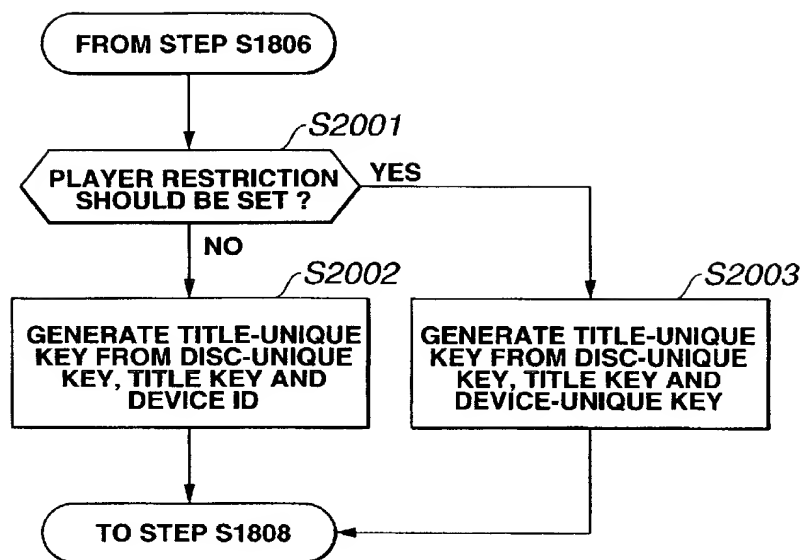
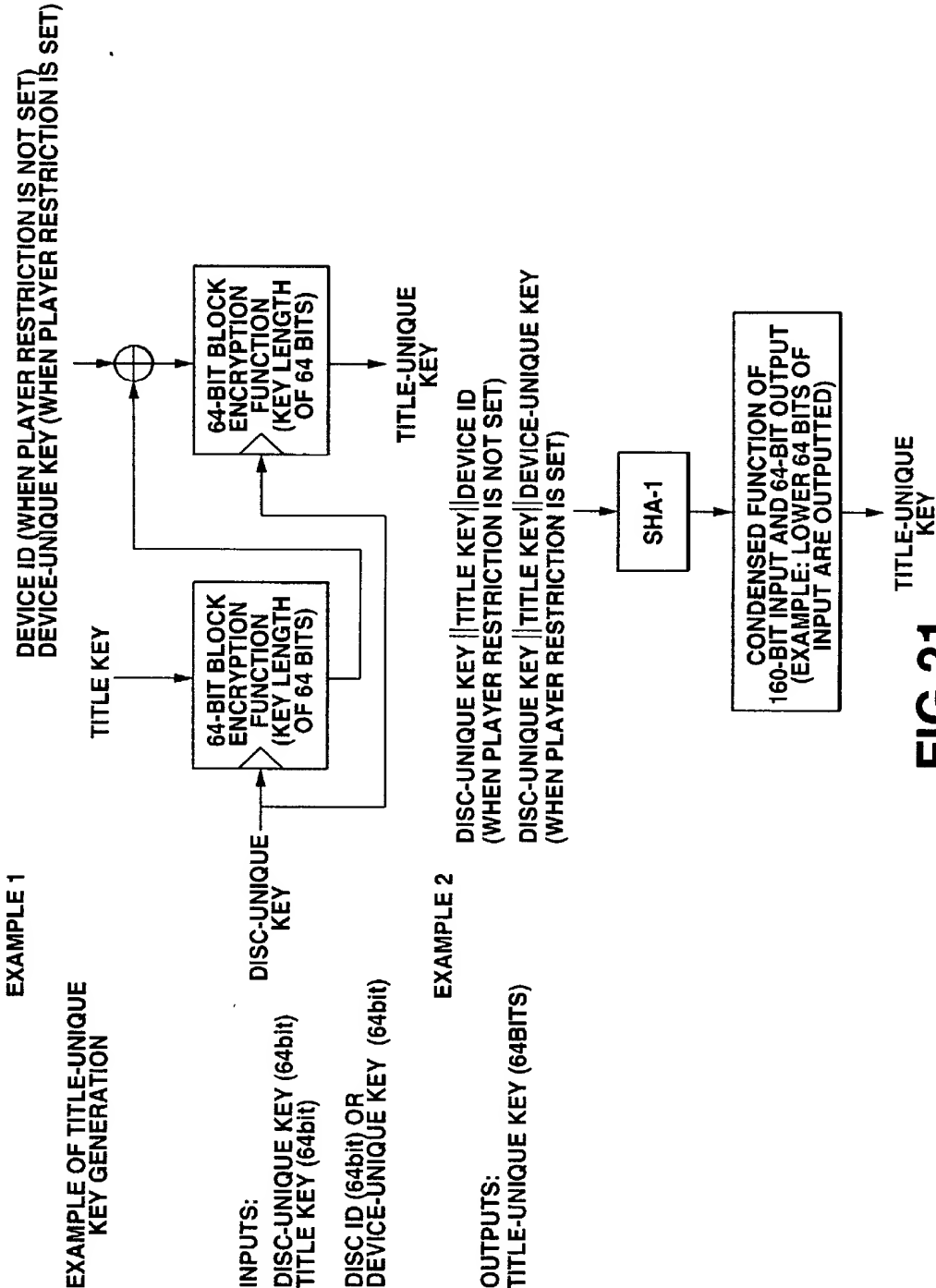
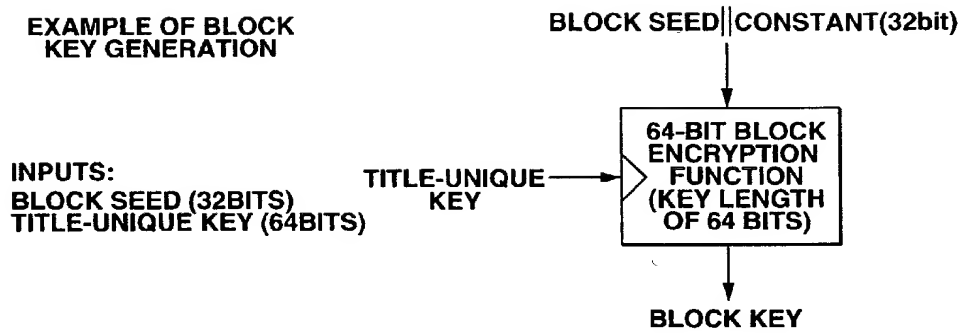


FIG.20



22/43

EXAMPLE 1

EXAMPLE OF BLOCK
KEY GENERATION

OUTPUTS:
BLOCK KEY (64BITS)

EXAMPLE 2

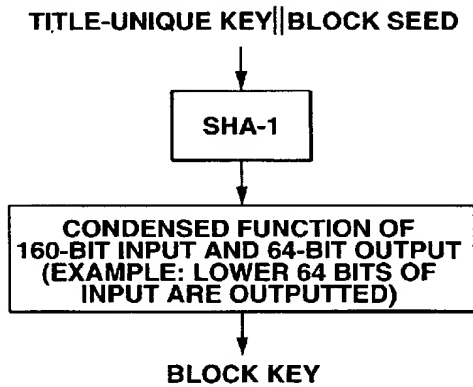


FIG.22



FIG. 23

24/43

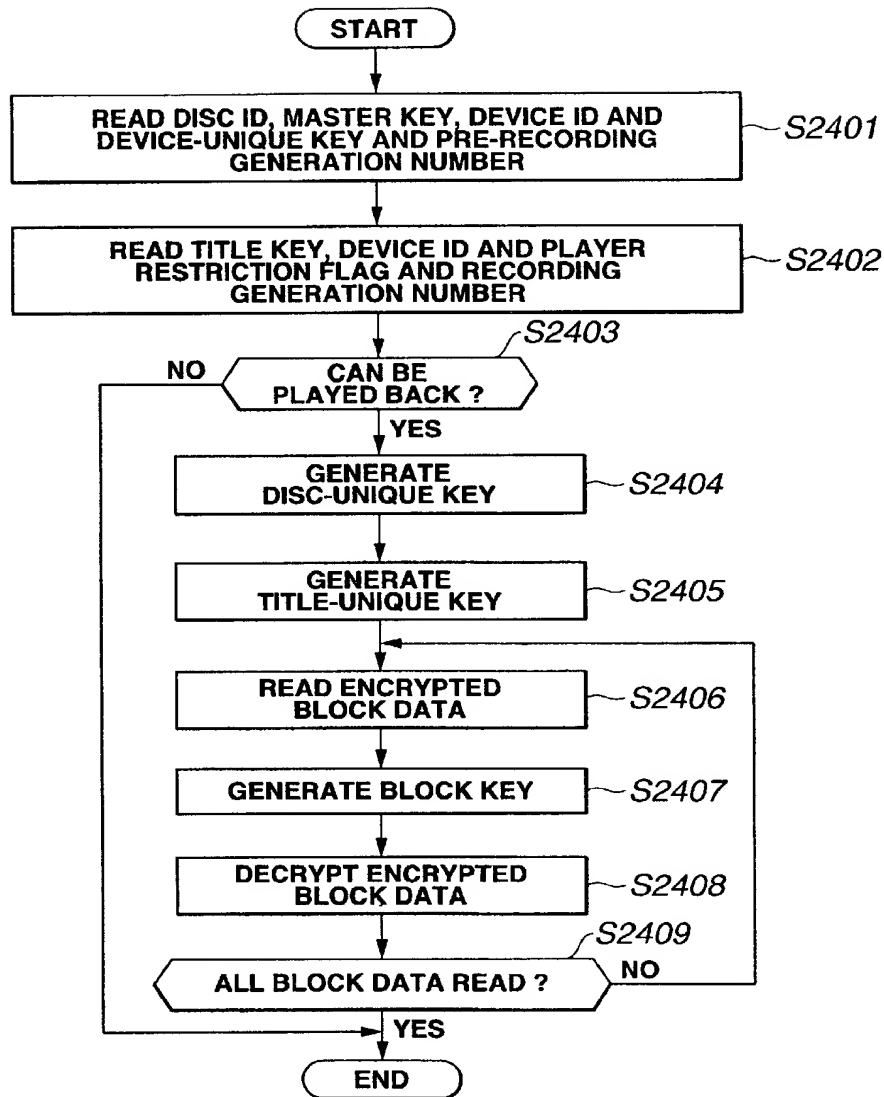


FIG.24

25/43

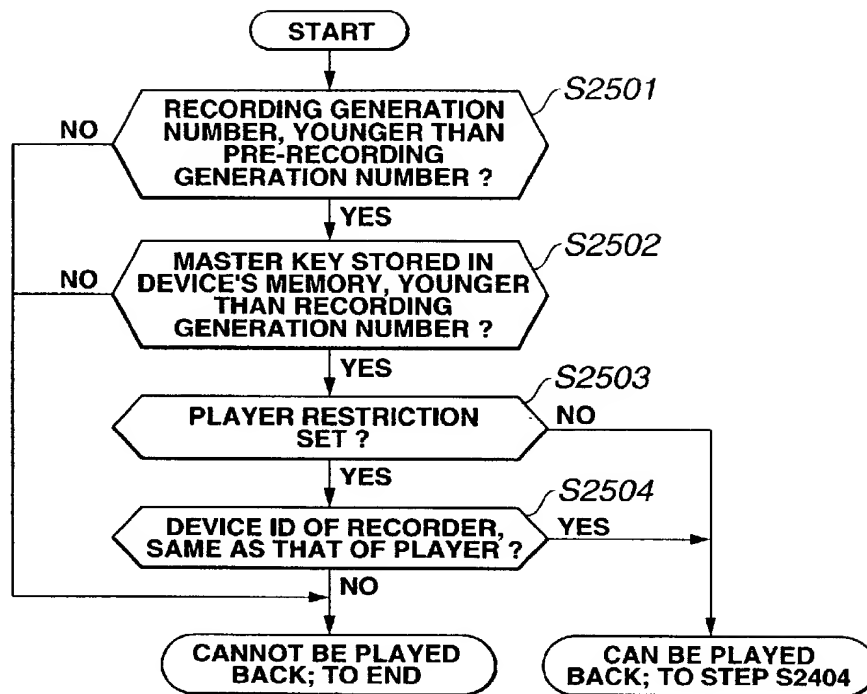


FIG.25

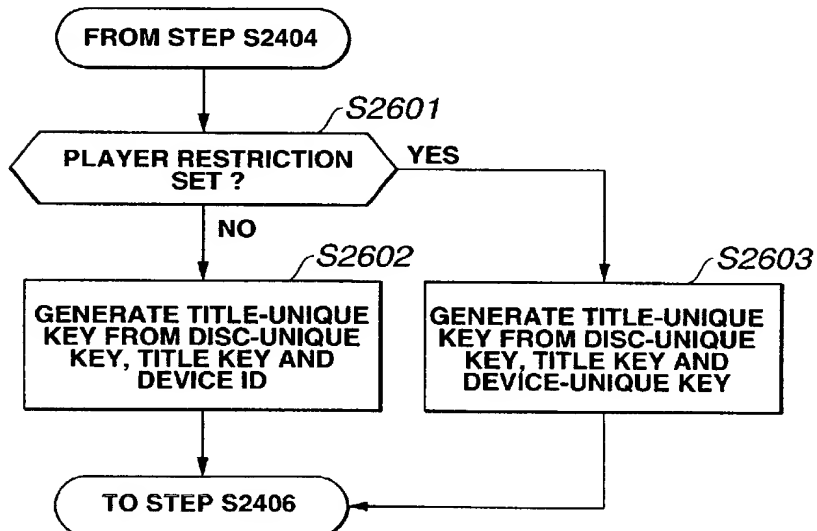


FIG.26

27/43

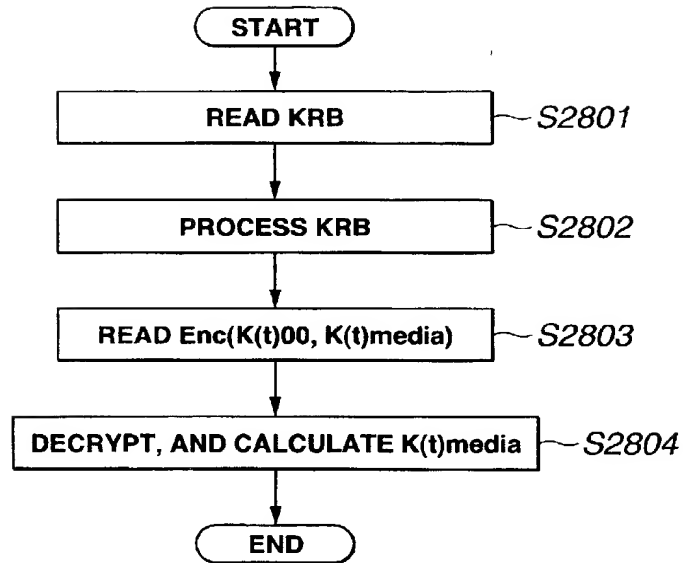


FIG.28

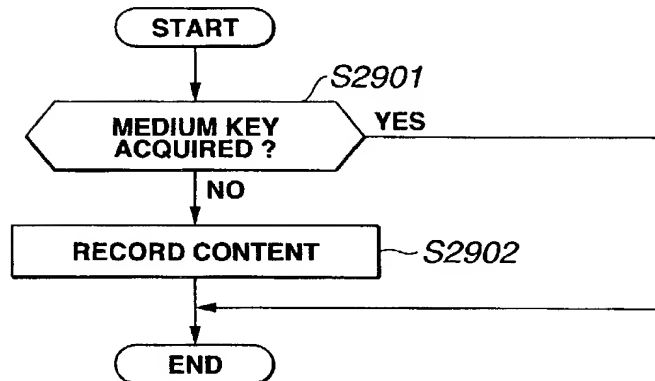


FIG.29



FIG. 31

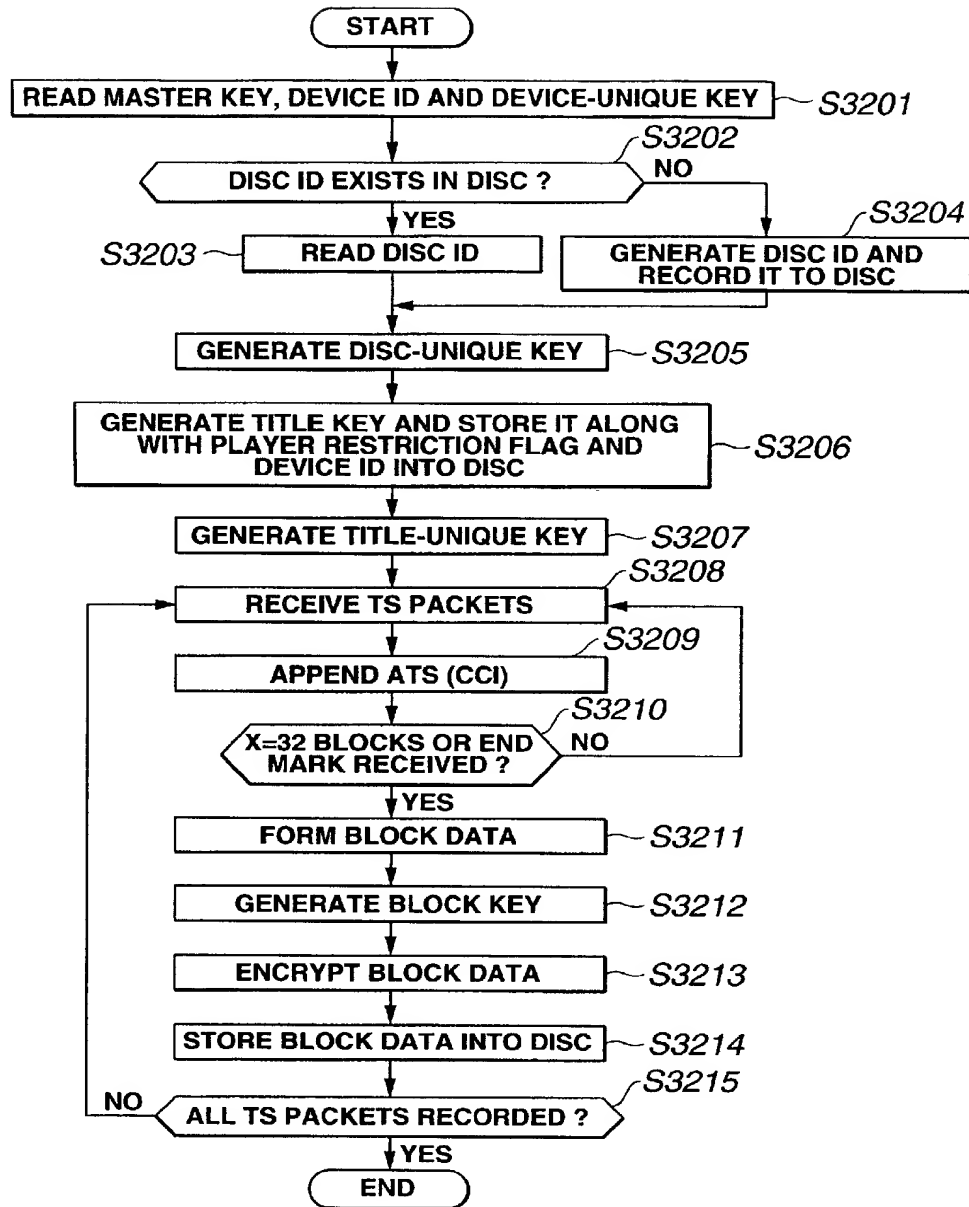


FIG.32



FIG. 33

32/43

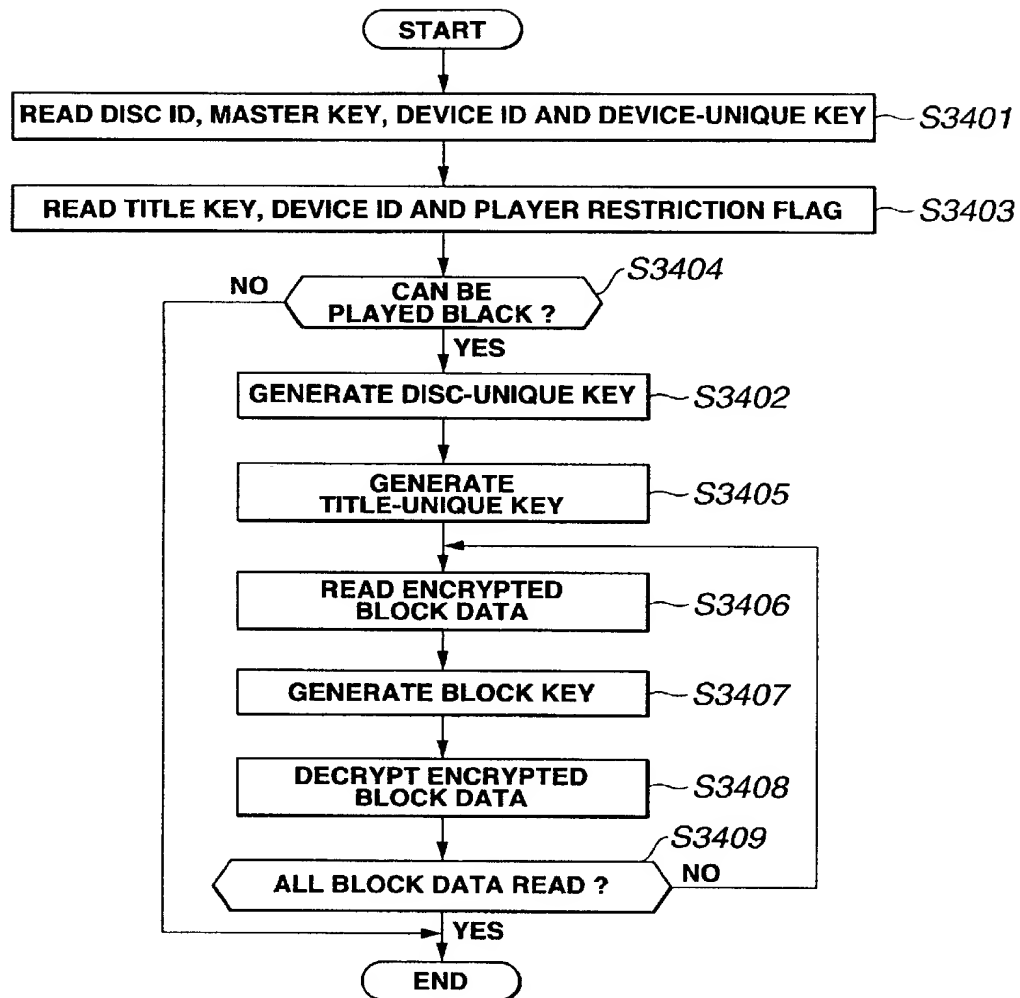


FIG.34

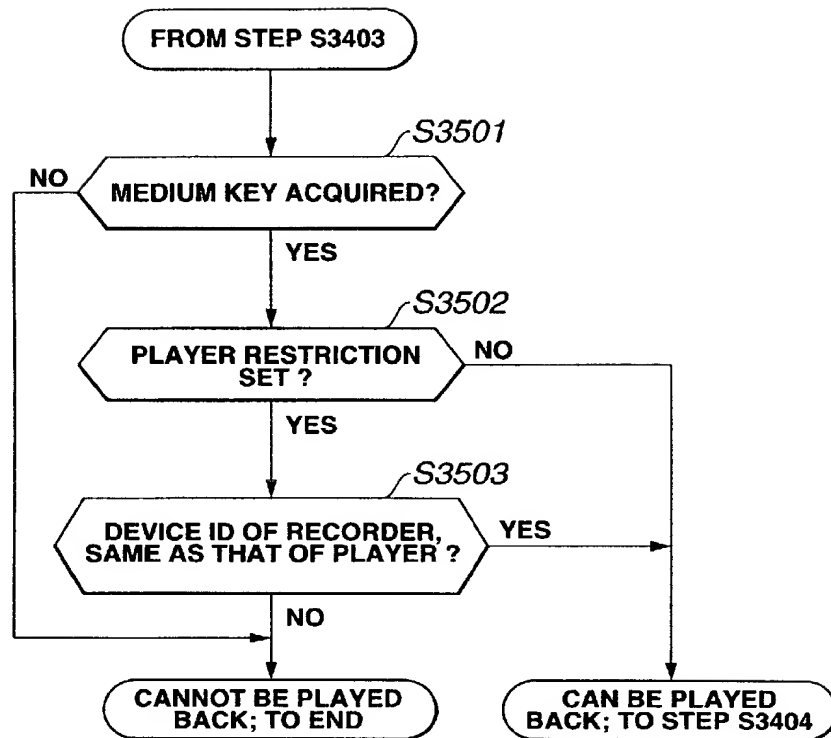


FIG.35

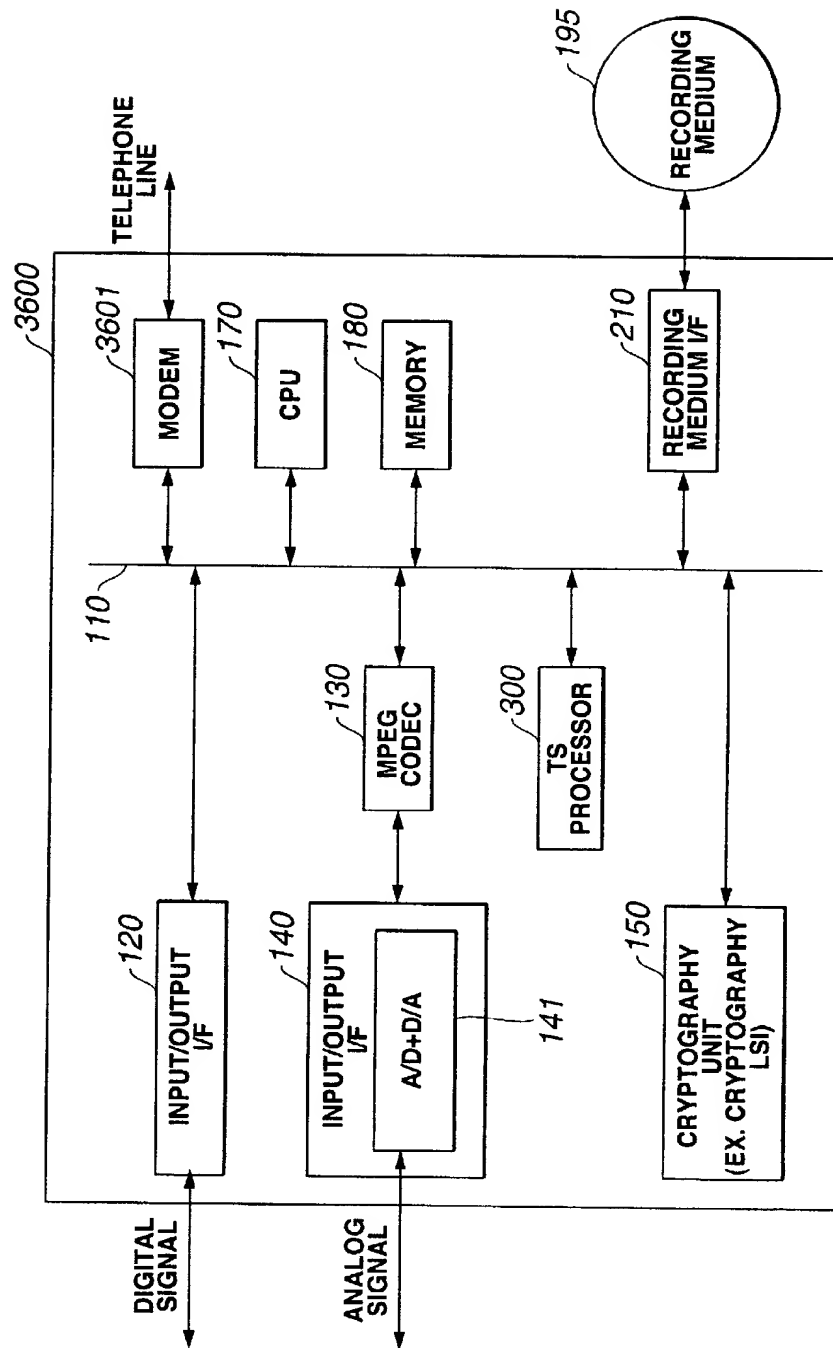


FIG.36

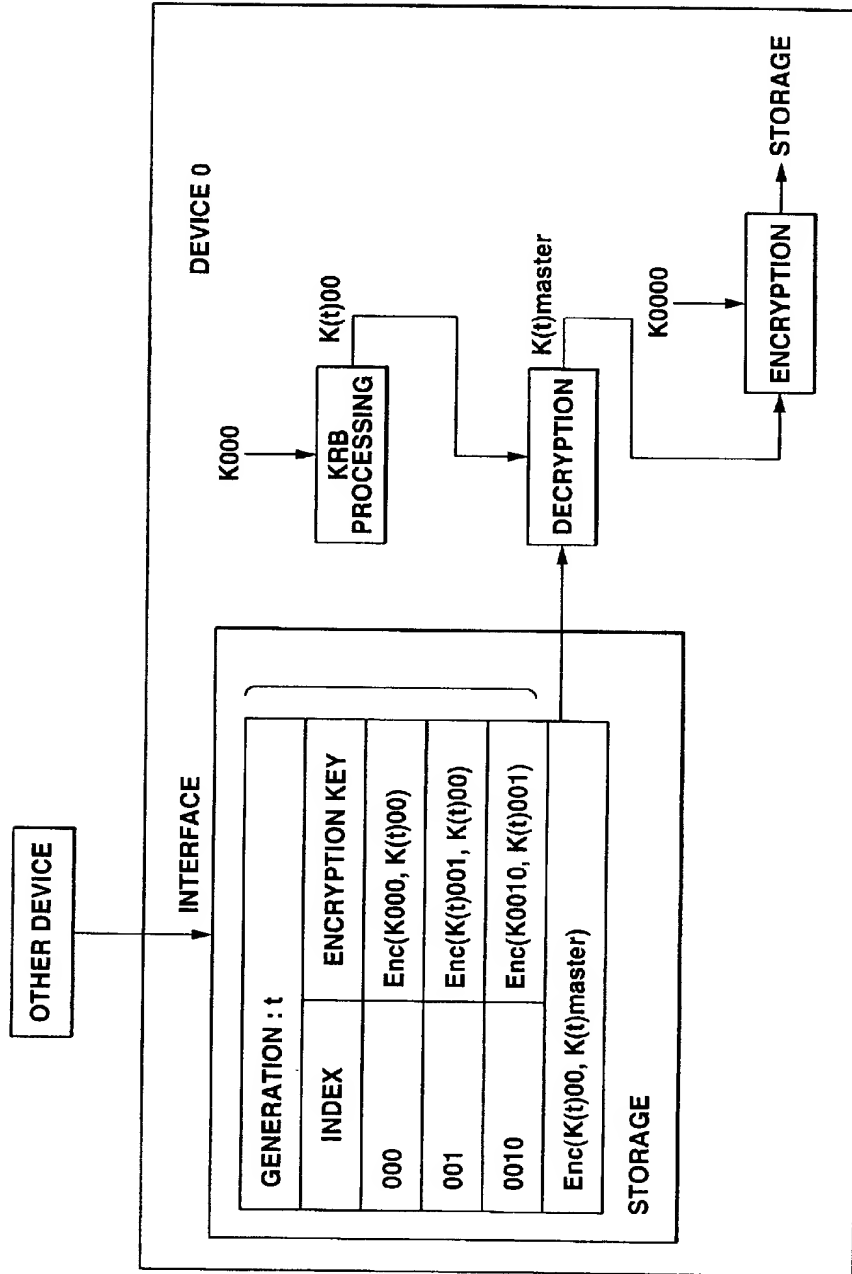


FIG.37

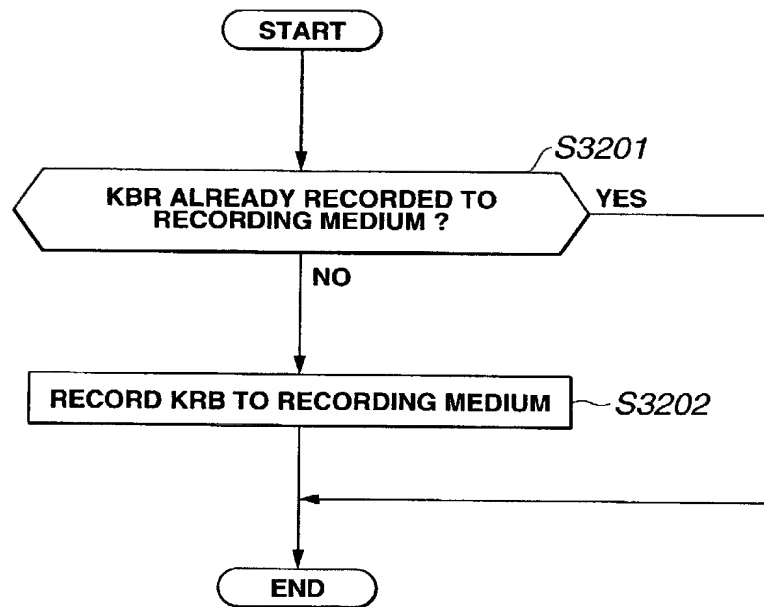


FIG.38

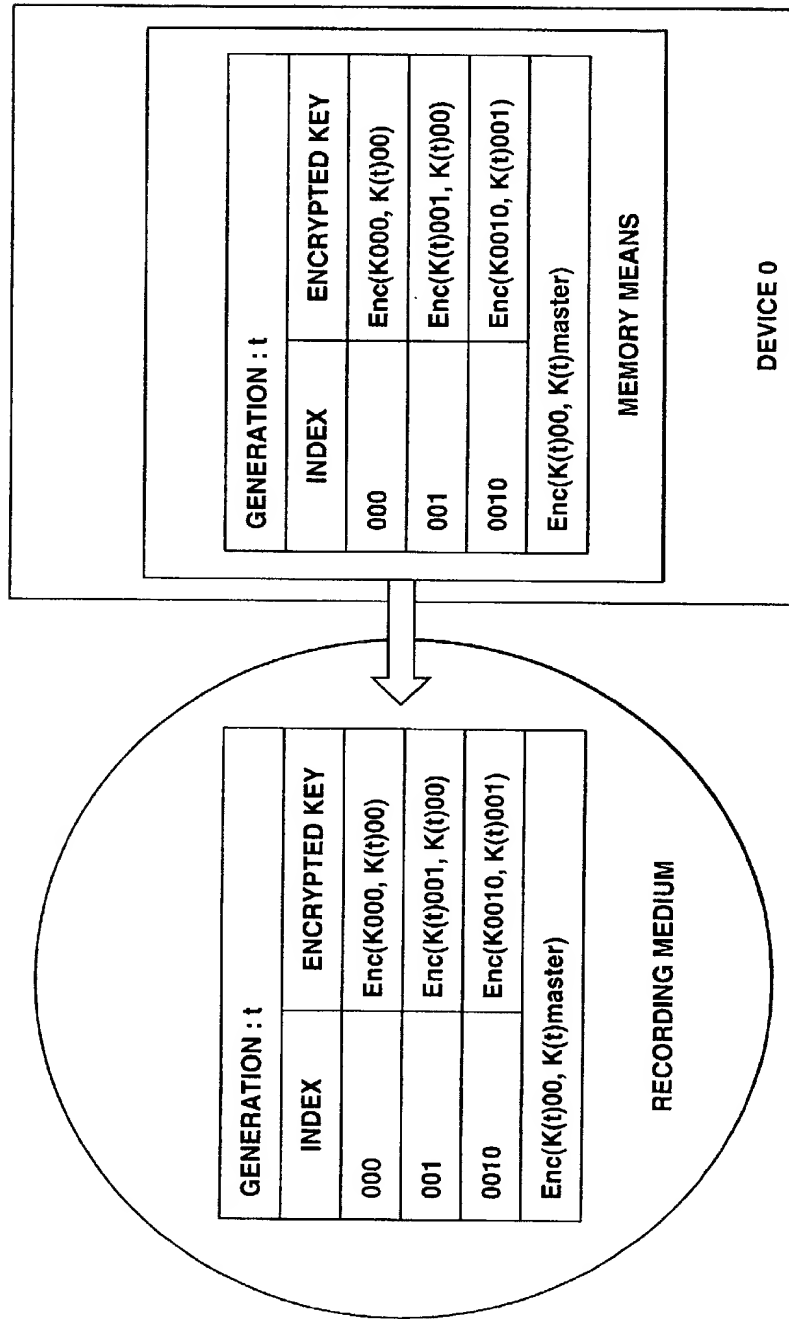


FIG.39

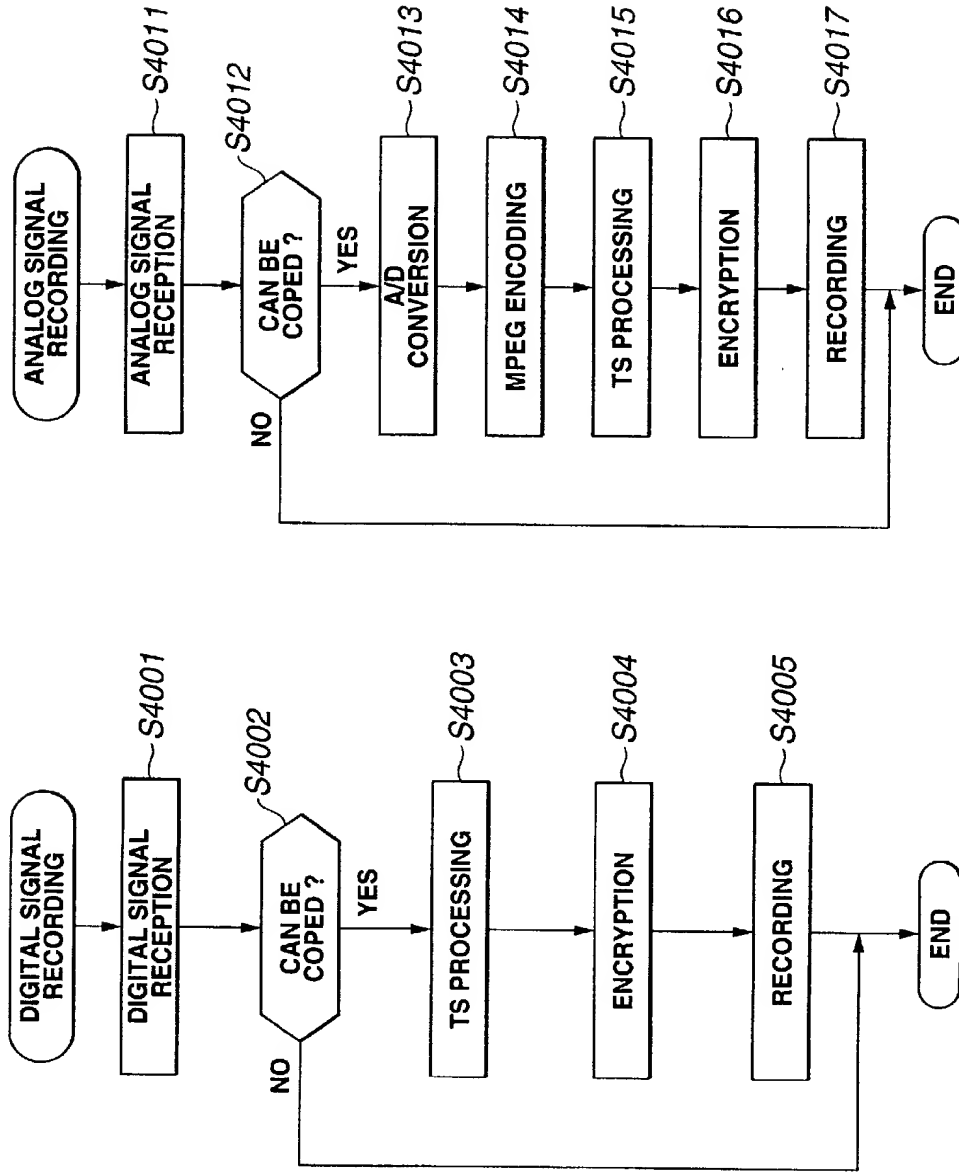


FIG.40B

FIG.40A

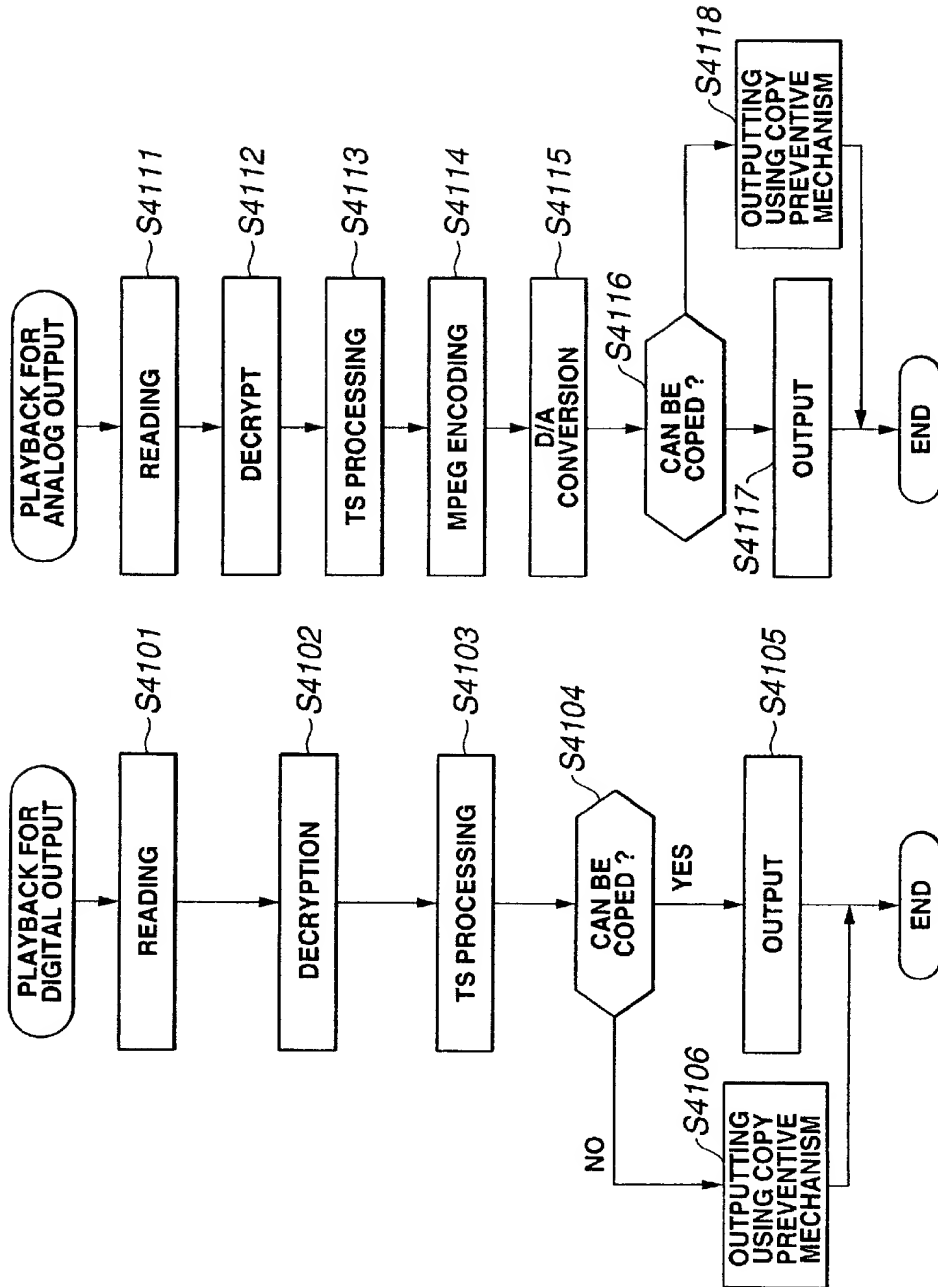


FIG.41B

FIG.41A

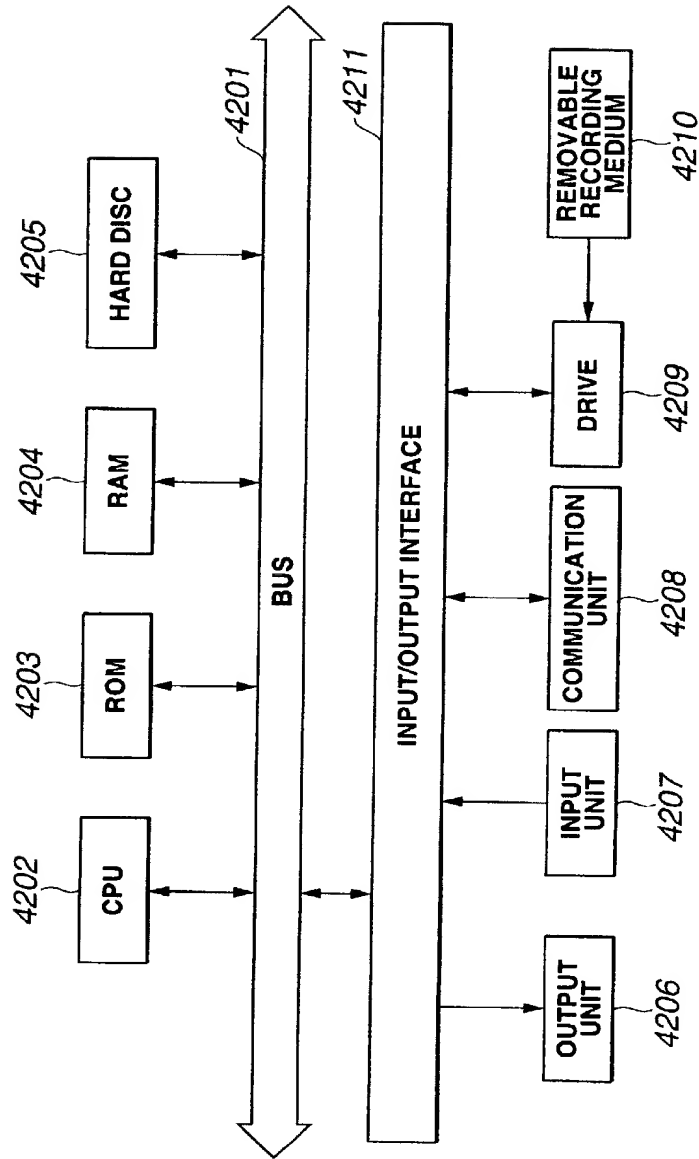


FIG.42

41/43

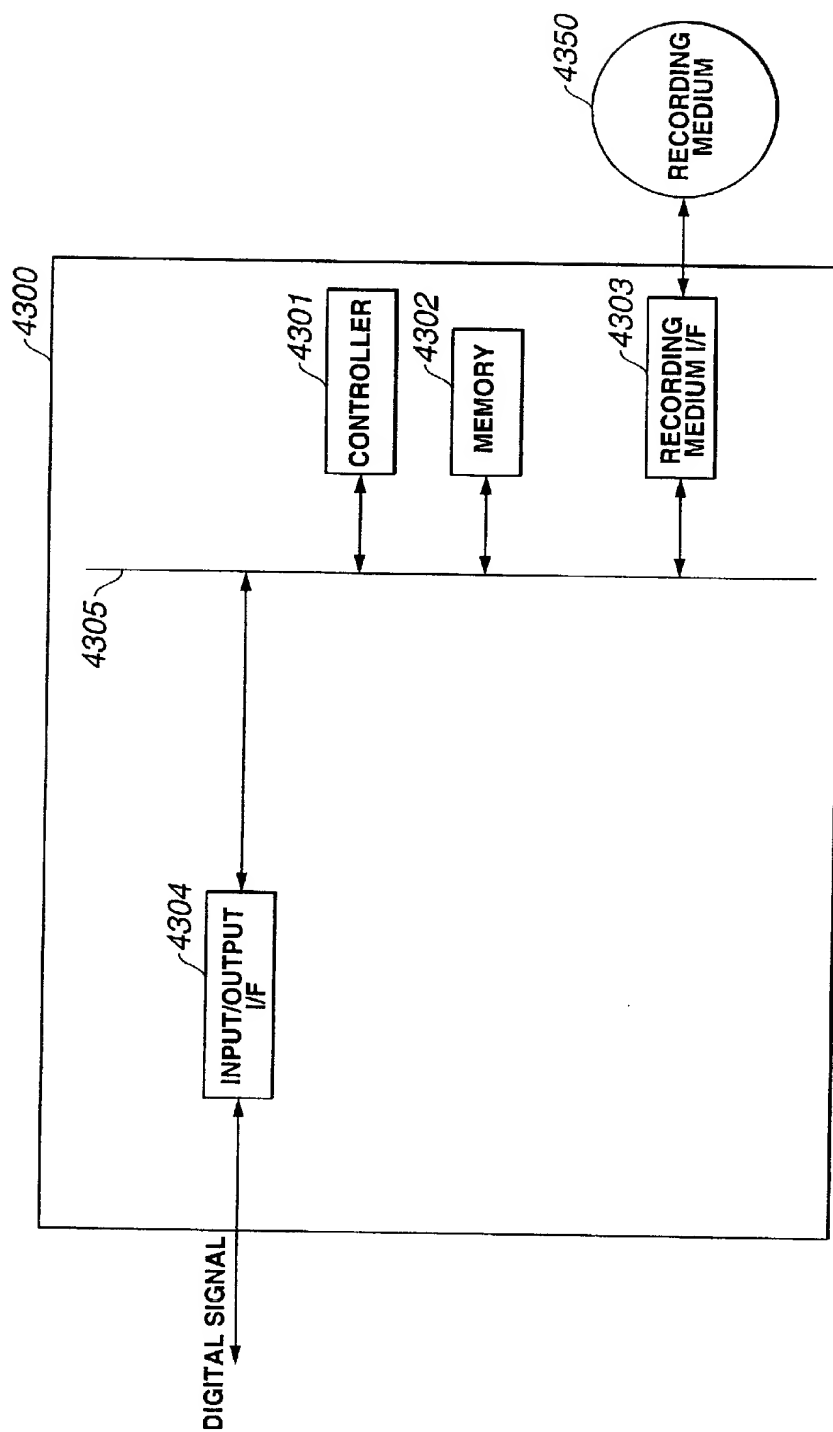


FIG.43

42/43

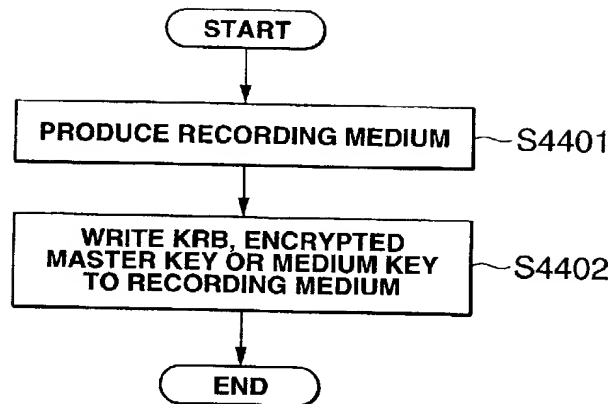


FIG.44

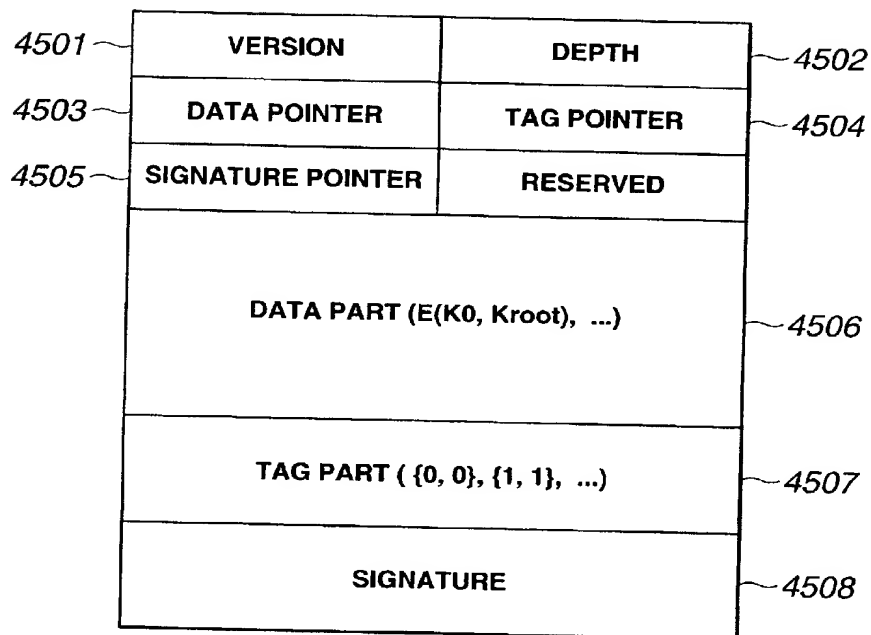


FIG.45

FIG.46B

KRB (KEY RENEWAL BLOCK)

NODE KEY OF VERSION:t IS SENT TO DEVICES 0, 1 AND 2

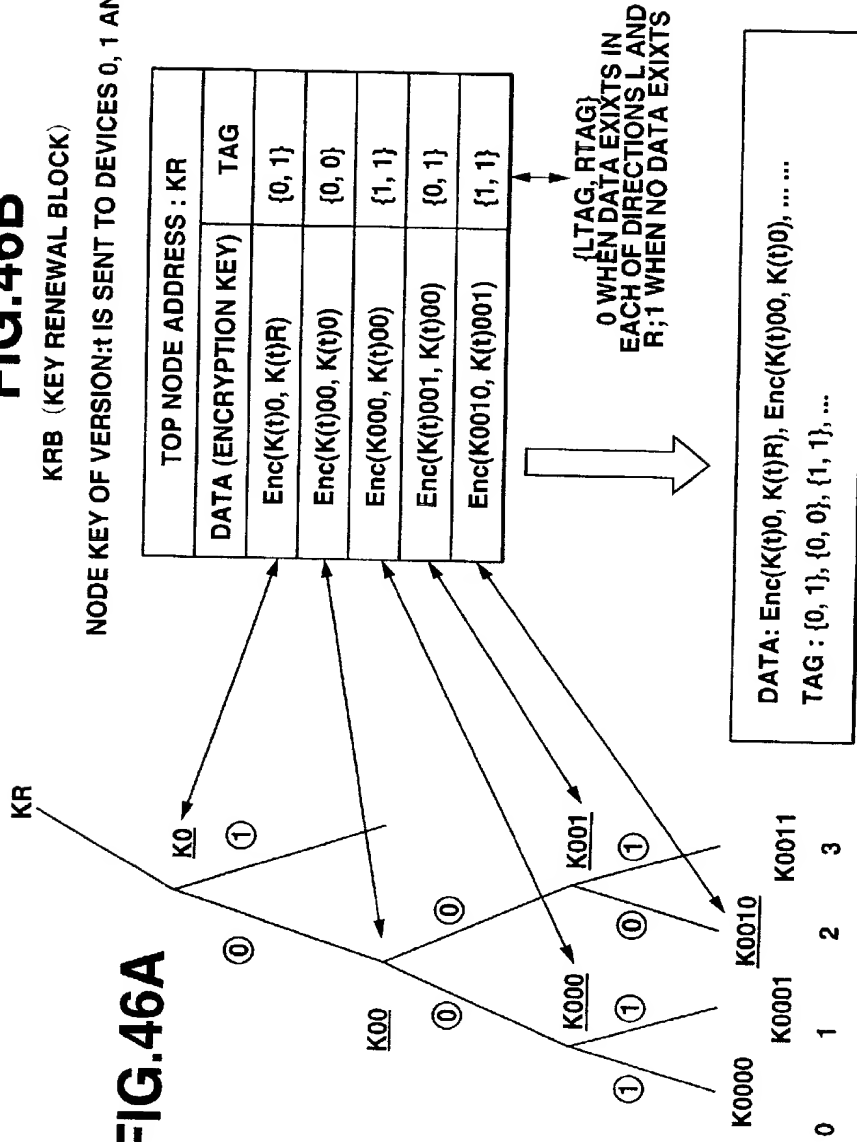


FIG.46C